UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF SOUTH CAROLINA
CHARLESTON DIVISION

CHRISTOPHER HART, individually and all others similarly situated, Plaintiff, v. SOUTHSTATE BANK, N.A., a company, SOUTHSTATE CORPORATION, a corporation, Defendants.	CASE NO. 2:24-cv-01905-RMG **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

For the Class Action Complaint, Plaintiff Christopher Hart, on behalf of himself and all others similarly situated, allege the following against Defendants SouthState Bank, N.A. ("SouthState Bank") and SouthState Corporation (collectively "Defendants"), based on personal knowledge as to Plaintiff and Plaintiff's own acts and on information and belief as to all other matters based upon, *inter alia*, the investigation conducted by and through Plaintiff's undersigned counsel:

SUMMARY OF THE CASE

1. SouthState Bank is a nationally-chartered bank that provides banking and financial products and services.

2. As part of SouthState Bank's business of offering banking and financial products and services, SouthState Bank collects personal data from customers, including but not limited to: names, addresses, dates of birth, and Social Security numbers, and financial account numbers. This personal information, is collectively referred to herein as "personally identifiable information"

("PII" or "Private Information").

3. This case involves the cybersecurity incident SouthState Bank announced on February 9, 2024, wherein the Private Information of SouthState Bank's current and former customers was exposed due to a flaw in SouthState Bank's information technology ("IT") systems, which allowed an unauthorized individual to access some of SouthState Bank's folders in its network and steal customer Private Information for unsavory and illegal purposes ("Data Breach").

4. This Class Action Complaint is filed on behalf of all persons in the United States, described more fully in the following sections, whose Private Information was compromised in the Data Breach.

JURISDICTION AND VENUE

5. This Court has jurisdiction over this action pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs, there are more than 100 class members, and at least one Class Member is a citizen of a state that differ from Defendants.

6. Venue is likewise proper in this District as to Defendants under 28 U.S.C. § 1391(a)(1) because a substantial part of the events or omissions giving rise to the claims asserted herein occurred in this District. Defendants conduct business through this District.

PARTIES

A. Plaintiff Christopher Hart

7. Plaintiff Christopher Hart is a resident and citizen of South Carolina. Plaintiff was a customer of SouthState Bank, entrusting SouthState Bank with safeguarding his Private Information.

B. Defendant SouthState Corporation

8. Defendant SouthState Corporation is a financial services company headquartered at 1101 First Street South, Suite 202 Winter Haven, Florida.

C. **Defendant SouthState Bank, N.A.**

9. Defendant SouthState Bank, N.A. is SouthState Corporation's subsidiary and nationally-chartered bank and provides consumer, commercial, mortgage, and wealth management services to millions of customers throughout Florida, Alabama, Georgia, North Carolina, South Carolina, and Virginia.

10. Defendant SouthState Bank is incorporated in South Carolina.

FACTUAL BACKGROUND

A. **The Data Breach**

11. As a part of providing banking and financial products and services, Defendant SouthState Bank requires that its customers provide sensitive Private Information, including but not limited to their: name, date of birth, phone number, address Social Security number, and financial account numbers.

12. On February 9, 2024, SouthState Corporation filed an 8-K report in front of the Securities and Exchange Commission ("SEC") publicly announcing for the first time the Data Breach, stating the following:

> SouthState Bank, N.A., (the "Company") detected what was determined to be a cybersecurity incident on February 6, 2024. Upon detection, the Company initiated its incident response and business continuity protocols and began taking measures to disrupt the unauthorized activity. As part of its process to address the incident, the Company proactively took measures to isolate parts of its network, which resulted in some disruption to the Company's business processes. The Company's operations have continued throughout this process in all material respects. The Company is conducting a thorough investigation and a cybersecurity firm has been engaged. Banking regulators and law enforcement have been notified.
>
> While the investigation is ongoing, as of the date of this filing, the incident has not had a material impact on the Company's operations, and the Company has not

> determined the incident is reasonably likely to materially impact the Company's financial conditions or results of operations.[1]

13. On March 29, 2024, SouthState Corporation filed an Amended Form 8-K, wherein it notified the SEC of the following:

> As disclosed in the Original Report, on February 6, 2024, SouthState Bank, N.A. detected what was determined to be a cybersecurity incident. Upon detection, SouthState initiated its incident response and business continuity protocols and began taking measures to disrupt the unauthorized activity. In addition, SouthState has been conducting an investigation. A cybersecurity firm was engaged to assist. SouthState also notified banking regulators and law enforcement. As a result of these and other measures, SouthState has contained the impact of the cybersecurity incident.
>
> Based on the investigation and findings, SouthState will mail notification letters to individuals whose personal information may have been involved.
>
> While the cybersecurity incident had a significant impact on certain of SouthState's business processes, as of the date of this filing, it has not had a material impact on SouthState's overall financial condition or results of operations, and SouthState has determined that the incident is not reasonably likely to have a material impact on its financial conditions or results of operations.[2]

14. On April 2, 2024, Defendant SouthState Bank began notifying Plaintiff and Class Members that it detected "unauthorized access to certain folders in our network" around February 6, 2024 and reported the unauthorized intrusion to government authorities and law enforcement.[3]

15. Among the types of Private Information compromised in the Data Breach are bank customers' names, Social Security numbers, and financial account numbers.[4]

16. Upon information and belief, over one million individuals were affected by the Data Breach.

---

[1] SouthState Corp., Current Report (Form 8-K) (Feb. 9, 2024).
[2] SouthState Corp., Current Report (Form 8-K/A) (Mar. 29, 2024).
[3] *SC bank customers are being notified about data breach earlier this year*, The Post and Courier (April 2, 2024), https://www.postandcourier.com/business/southstate-south-carolina-bank-cybersecurity-data-breach-florida-columbia/article_2ca858aa-f105-11ee-9016-97242bd1b844.html.
[4] *Id*.

17. Yet, SouthState Bank states the following on its "Consumer Privacy Notice" regarding its supposed commitment to safeguarding the personal information collected from current and former customers:

> Regardless of changes in technology and information, **SouthState has always been, and will continue to be, committed to the principles of customer privacy**. We understand that when you open an account with us, apply for a loan, or deal with us or one of our affiliated companies in any way, we ask you to provide us with private financial and personal information.
>
> **We honor the trust you place in us by maintaining the confidentiality and accuracy of that information, and we use it in manners consistent with the confidence you have placed in us. We will uphold both the letter and the spirit of federal and state laws as they relate to this important issue**.[5]

18. Despite SouthState Bank's supposed commitment to "maintaining the confidentiality and accuracy" of Plaintiff's and Class Member's Private Information, SouthState Bank still lacks the safeguards and protections for current and former customers' Private Information, and that information remains at risk today and into the future, until SouthState Bank is compelled to secure that Private Information.

B. **SouthState Bank Failed to Comply With FTC Requirements**

19. Federal and State governments have likewise established security standards and issued recommendations to temper data breaches and the resulting harm to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[6]

---

[5] *Consumer Privacy Notice*, SouthState Bank, N.A., https://www.southstatebank.com/global/privacy-notice (last accessed Apr. 4, 2024).

[6] *Start With Security*, Fed. Trade Comm'n (June 2015) https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Apr. 5, 2024).

20. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[7] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[8]

21. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiff and Class Members are long lasting and severe. Once stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

22. In *Protecting Personal Information: A Guide for Business*, the FTC established guidelines for fundamental data security principles and practices for business.[9] The guidelines note businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

[7] 17 C.F.R. § 248.201 (2013).
[8] *Id*.
[9] *Protecting Personal Information: A Guide for Business*, Fed. Trade Comm'n (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Apr. 5, 2024).

23. The FTC recommends that companies not maintain Private Information longer than is needed; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[10]

24. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

25. SouthState Bank's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

26. In this case, SouthState Bank was at all times fully aware of its obligation to protect the Private Information of its customers because of its participation in the storage of Private Information. SouthState Bank was also aware of the significant repercussions if it failed to do so because SouthState Bank collected Private Information from millions of customers daily and they knew that this data, if hacked, would result in injury to consumers, including Plaintiff and Class members.

27. Despite understanding the consequences of inadequate data security, SouthState Bank failed to take appropriate protective measures to protect and secure customer's Private Information, including Plaintiff and Class members.

[10] *Start With Security*, *supra* n. 6.

28. Despite understanding the consequences of inadequate data security, SouthState Bank operated computer network systems with outdated operating systems and software; failed to enable point-to-point and end-to-end encryption; failed to detect an intrusion dating back to February 2024; and, failed to take other measures necessary to protect its IT systems.

29. Upon information and belief, SouthState Bank collects, stores, and maintains the Private Information of all customers who purchase products and services from SouthState Bank.

C. **SouthState Bank Failed to Follow Data Security Industry Standards**

30. Various cybersecurity industry best practices have been published and should be consulted as a go-to resource when developing an organization's cybersecurity standards. The Center for Internet Security ("CIS") promulgated its Critical Security Controls, which identify the most commonplace and essential cyber-attacks that affect businesses every day and proposes solutions to defend against those cyber-attacks. All organizations collecting and handling PII, such as Defendants, are strongly encouraged to follow these controls.

31. Further, the CIS Benchmarks are the overwhelming option of choice for auditors worldwide when advising organizations on the adoption of a secure build standard for any governance and security initiative, including PCI DSS, NIST 800-53, SOX, FISMA, ISO/IEC 27002, Graham Leach Bliley and ITIL.

32. Several best practices have been identified that a minimum should be implemented by companies like Defendants, including but not limited to securely configuring business software, managing access controls and vulnerabilities to networks, systems, and software, maintaining network infrastructure, defending networks, adopting data encryption while data is both in transit and at rest, and securing application software.

33. Defendants failed to follow these and other industry standards to adequately protect the Private Information of Plaintiff and Class Members.

D. **Private Information is Extremely Valuable**

34. The types of information compromised in the Data Breach are highly valuable to identity thieves. Names and Social Security numbers can be used to gain access to a variety of existing accounts.

35. Identity thieves can also use the Private Information to harm Plaintiff and Class members through embarrassment, blackmail, or harassment in person or online, or to commit other types of fraud including obtaining ID cards or driver's licenses, fraudulently obtaining tax returns and refunds, and obtaining government benefits. A Presidential Report on identity theft states that:

> In addition to the losses that result when identity thieves fraudulently open accounts or misuse existing accounts, . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.
>
> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.[11]

36. The problems associated with identity theft are exacerbated by the fact that many identity thieves will wait years before attempting to use the Private Information they have obtained.

[11] *The President's Identity Theft Task Force, Combating Identity Theft: A Strategic Plan*, Fed. Trade Comm'n (Apr. 2007), http://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-plan/strategicplan.pdf.

Indeed, in order to protect themselves, Class Members will need to remain vigilant against unauthorized data use for years and decades to come.

37. Once stolen, Private Information can be used in a number of different ways. One of the most common is that it is offered for sale on the "dark web," a heavily encrypted part of the Internet that makes it difficult for authorities to detect the location or owners of a website. The dark web is not indexed by normal search engines such as Google and is only accessible using a Tor browser (or similar tool), which aims to conceal users' identities and online activity. The dark web is notorious for hosting marketplaces selling illegal items such as weapons, drugs, and PII.[12] Websites appear and disappear quickly, making it a very dynamic environment.

38. Once someone buys Private Information, it is then used to gain access to different areas of the victim's digital life, including bank accounts, social media, and credit card details. During that process, other sensitive data may be harvested from the victim's accounts, as well as from those belonging to family, friends, and colleagues.

E. The Data Breach Caused Harm and Will Result in Additional Fraud

39. Without detailed disclosure to SouthState Bank's current and former customers, they, including Plaintiff and Class Members, were unknowingly and unwittingly left exposed to continued misuse and ongoing risk of misuse of their Private Information for months, without being able to take necessary precautions to prevent imminent harm.

40. The ramifications of SouthState Bank's failure to keep Plaintiff's and Class Members' data secure are severe.

[12] Brian Hamrick, *The dark web: A trip into the underbelly of the internet*, WLWT News (Feb. 9, 2017), http://www.wlwt.com/article/the-dark-web-a-trip-into-the-underbelly-of-the-internet/8698419.

41. Consumer victims of data breaches are much more likely to become victim of identity fraud. This conclusion is based on an analysis of four years of data that correlated each year's data breach victims with those who also reported being victims of identity fraud.[13]

42. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[14] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person."[15]

43. Private Information is a valuable commodity to identity thieves once the information has been compromised. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[16]

44. Identity thieves can use Private Information, such as that of Plaintiff and Class Members, which SouthState Bank failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

45. Analysis of a 2016 survey of 5,028 consumers found "The quicker a financial institution, credit card issuer, wireless carrier or other service provider is notified that fraud has occurred on an account, the sooner these organizations can act to limit the damage. Early

---

[13] *2022 True Cost of Fraud Study*, LexisNexis, https://risk.lexisnexis.com/-/media/files/financial%20services/research/lnrs_true_cost_of_fraud_retail_ecommercev3-2022_research_nxr15605-00-0822-en-us.pdf, (last visited Apr. 5, 2024).
[14] 17 C.F.R § 248.201 (2013).
[15] *Id.*
[16] *Fighting Identity Theft with the Red Flags Rule: A How-To Guide for Business*, Fed. Trade Comm'n (May 2013), https://www.ftc.gov/business-guidance/resources/fighting-identity-theft-red-flags-rule-how-guide-business.

notification can also help limit the liability of a victim in some cases, as well as allow more time for law enforcement to catch the fraudsters in the act."[17]

46. As a result of Defendants' delay in notifying consumers of the Data Breach, the risk of fraud for Plaintiff and Class Members has been driven even higher.

47. Javelin Strategy and Research reports that identity thieves stole over $20 billion worth of Private Information in 2022.[18]

48. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that identity theft victims reported spending "a mean of 7 hours resolving problems[]" in 2021.[19]

49. An independent financial services industry research study conducted for BillGuard—a private enterprise that automates the consumer task of finding unauthorized transactions that might otherwise go undetected—calculated the average per-consumer cost of all unauthorized transactions at roughly US $215 per cardholder incurring these charges,[20] some portion of which could go undetected and thus must be paid entirely out-of-pocket by consumer victims of account or identity misuse.

[17] *Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study*, Javelin (Feb. 1, 2017), https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new.

[18] *See* John Buzzard, *2023 Identity Fraud Study: The Butterfly Effect*, Javelin (Mar. 28, 2023), https://javelinstrategy.com/research/2023-identity-fraud-study-butterfly-effect.

[19] *Victims of Identity Theft*, Bureau of Justice Statistics (Oct. 2023), https://bjs.ojp.gov/document/vit21.pdf.

[20] Hadley Malcom, *Consumers rack up $14.3 billion in gray charges*, USAToday (July 25, 2013), https://www.usatoday.com/story/money/personalfinance/2013/07/25/consumers-unwanted-charges-in-billions/2568645/.

50. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[21]

51. Thus, Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiff and the Class are incurring and will continue to incur such damages in addition to any fraudulent credit and debit card charges incurred by them and the resulting loss of use of their credit and access to funds.

F. **Plaintiff and Class Members Suffered Damages**

a. Plaintiff Christopher Hart

52. Plaintiff has not been a customer of SouthState Bank since he closed his bank account with SouthState Bank ten (10) years ago. Thus, SouthState Bank has retained his Private Information for nearly a decade longer than needed.

53. On or about April 3, 2024, Plaintiff Hart received a letter from Defendant notifying him that his Private Information—including, *inter alia*, his name, Social Security number, and financial account information—was compromised on or about February 2024.

54. Following the Data Breach, Plaintiff Hart was the victim of debit/credit card fraud.

55. On or about February 27, 2024, Plaintiff Hart was notified by American Express of charges on his card not authorized by Plaintiff.

[21] Report to Congressional Requesters, GAO at 29 (June 2007), http://www.gao.gov/new.items/d07737.pdf.

56. After being notified of the unauthorized charges, Plaintiff Hart was forced to cancel his American Express card and obtain a new card.

57. Upon information and belief, after the Data Breach, Plaintiff Hart was notified by a credit monitoring agency that his Private Information was on the "dark web."

58. Following the Data Breach, Plaintiff Hart noticed an increase in spam emails, text messages, and/or phone calls.

59. Plaintiff Hart has spent time and effort dealing with and mitigating the consequences of the Data Breach.

60. Upon information and belief, Plaintiff Hart spent over five (5) hours dealing with the consequences of the Data Breach. The time spent by Plaintiff consisted of researching the events surrounding the Data Breach, verifying the unauthorized charges on his old American Express card, coordinating with American Express to cancel his old card and order a new card, and monitoring his bank accounts, credit card accounts, and credit score.

61. From the Data Breach, Plaintiff Hart has and continues to suffer emotional distress, for he has trouble sleeping from researching developments on the Data Breach and protecting his accounts from potential fraud.

b. The Nationwide Class

62. The Private Information of Plaintiff and Class Members is private and sensitive in nature and was left inadequately protected by SouthState Bank. SouthState Bank did not obtain Plaintiff's and Class Members' consent to disclose their Private Information to any other person as required by applicable law and industry standards.

63. The Data Breach was a direct and proximate result of SouthState Bank's failure to properly safeguard and protect Plaintiff's and Class members' Private Information from

unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including SouthState Bank's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class Members' Private Information to protect against reasonably foreseeable threats to the security or integrity of such information.

64. Upong information and belief, SouthState Bank had the resources to prevent a breach. SouthState Bank neglected to adequately invest in data security, despite the growing number of data intrusions and several years of well-publicized data breaches.

65. Had SouthState Bank remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, SouthState Bank would have prevented intrusion into its information storage and security systems and, ultimately, the theft of its customers' confidential Private Information.

66. As a direct and proximate result of SouthState Bank's wrongful actions and inaction and the resulting Data Breach, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports. This time has been lost forever and cannot be recaptured.

67. SouthState Bank's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff's and Class Members' Private

Information, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. theft of their personal and financial information;

b. unauthorized charges on their debit and credit card accounts;

c. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their credit/debit card and personal information being placed in the hands of criminals and misused via the sale of Plaintiff's and Class Members' information on the Internet's black market;

d. the untimely and inadequate notification of the Data Breach;

e. the improper disclosure of their Private Information;

f. loss of privacy;

g. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

h. ascertainable losses in the form of deprivation of the value of their Private Information, for which there is a well-established national and international market;

i. ascertainable losses in the form of the loss of cash back or other benefits as a result of their inability to use certain accounts and cards affected by the Data Breach;

j. loss of use of, and access to, their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse credit notations; and,

k. the loss of productivity and value of their time spent to address, attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the inconvenience, nuisance and annoyance of dealing with all such issues resulting from the Data Breach.

68. While Plaintiff's and Class Members' Private Information have been stolen, SouthState Bank continues to hold consumers' Private Information, including Plaintiff's and Class members'. Particularly because SouthState Bank has demonstrated an inability to prevent a breach or stop it from continuing even after being detected, Plaintiff and Class Members have an undeniable interest in ensuring that their PII is secure, remains secure, is properly and promptly destroyed, and is not subject to further theft.

CLASS ACTION ALLEGATIONS

69. Pursuant to Rule 23(b)(2), (b)(3) and (c)(4) of the Federal Rules of Civil Procedure, Plaintiff, individually and on behalf of all others similarly situated, brings this lawsuit on behalf of himself and as a class action on behalf of the following Classes:

> **Nationwide Class**: All persons in the United States who provided Private Information to SouthState Bank and whose Private Information was accessed, compromised, or stolen from SouthState Bank in the Data Breach.
> **South Carolina Subclass**: All persons in South Carolina who provided Private Information to SouthState Bank and whose Private Information was accessed, compromised, or stolen from SouthState Bank in the Data Breach.

70. Excluded from the Class are Defendants and any entities in which any Defendant or their subsidiaries or affiliates have a controlling interest, and Defendants' officers, agents, and

employees. Also excluded from the Class are the judge assigned to this action, members of the judge's staff, and any member of the judge's immediate family.

71. **Numerosity:** The members of each Class are so numerous that joinder of all members of any Class would be impracticable. The exact number and names and addresses of Class members are identifiable through documents maintained by Defendants.

72. **Commonality and Predominance:** This action involves common questions of law or fact, which predominate over any questions affecting individual Class members, including:

i. Whether Defendants represented to the Class that they would safeguard Class members' PII;

ii. Whether Defendants owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;

iii. Whether Defendants breached a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;

iv. Whether Class members' PII was accessed, compromised, or stolen in the Data Breach;

v. Whether Defendants knew about the Data Breach before it was announced to the public and Defendants failed to timely notify the public of the Data Breach;

vi. Whether Defendants' conduct violated § 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, *et seq.*,

vii. Whether Plaintiff and the Class are entitled to equitable relief, including, but not limited to, injunctive relief and restitution; and

viii. Whether Plaintiff and the other Class members are entitled to actual, statutory, or other forms of damages, and other monetary relief.

73. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous common questions that dominate this action.

74. **Typicality:** Plaintiff's claims are typical of the claims of the other members of their respective classes because, among other things, Plaintiff and the other Class members were injured through the substantially uniform misconduct by Defendants. Plaintiff is advancing the same claims and legal theories on behalf of themselves and all other Class members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of other Class members arise from the same operative facts and are based on the same legal theories.

75. **Adequacy of Representation:** Plaintiff is an adequate representative of the classes because his interests do not conflict with the interests of the other Class members he seeks to represent; he has retained counsel competent and experienced in complex class action litigation and Plaintiff will prosecute this action vigorously. The Class members' interests will be fairly and adequately protected by Plaintiff and his counsel.

76. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiff and the other members of their respective classes are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendants, making it impracticable for Class members to individually seek redress for Defendants' wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments, and increase the delay and expense to all parties and the

court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

77. Further, Defendants have acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the members of the Class as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

78. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Class members' PII was accessed, compromised, or stolen in the Data Breach;

b. Whether (and when) Defendants knew about any security vulnerabilities that led to the Data Breach before it was announced to the public and whether Defendants failed to timely notify the public of those vulnerabilities and the Data Breach;

c. Whether Defendants' representations that it would secure and protect the PII of Plaintiff and members of the classes were facts that reasonable persons could be expected to rely upon when deciding whether to use Defendants' services or purchase Defendants' products;

d. Whether Defendants misrepresented the safety of its many systems and services, specifically the security thereof, and its ability to safely store Plaintiff's and Class members' PII;

e. Whether Defendants concealed crucial information about its inadequate data security measures from Plaintiff and the Class;

f. Whether Defendants failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

g. Whether Defendants knew or should have known that it did not employ reasonable measures to keep Plaintiff's and Class members' PII secure and prevent the loss or misuse of that information;

h. Whether Defendants failed to "implement and maintain reasonable security procedures and practices" for Plaintiff's and Class members' PII in violation of Section 5 of the FTC Act;

i. Whether Defendants failed to provide timely notice of the Data Breach in violation of state consumer protection laws, including S.C. Code Ann. §§ 39-1-90;

j. Whether Defendants owed a duty to Plaintiff and the Class to safeguard their PII and to implement adequate data security measures;

k. Whether Defendants breached that duty;

l. Whether such representations were false with regard to storing and safeguarding Plaintiff's and Class members' PII; and

m. Whether such representations were material with regard to storing and safeguarding Class members' PII.

CAUSES OF ACTION

COUNT I – NEGLIGENCE
(On behalf of Plaintiff and the Class)

79. Plaintiff repeats, realleges, and incorporates by reference the allegations contained in paragraphs 1 through 78 as though fully stated herein.

80. Defendants owed a duty to Plaintiff and the Class to exercise reasonable care in safeguarding and protecting their Private Information and keeping it from being compromised, lost, stolen, misused, and or/disclosed to unauthorized parties. This duty included, among other things, designing, maintaining, and testing Defendants' security systems to ensure the Private Information of Plaintiff and the Class was adequately secured and protected, including using encryption technologies. Defendants further had a duty to implement processes that would detect a breach of its security system in a timely manner.

81. Defendants knew that the Private Information of Plaintiff and the Class was personal and sensitive information that is valuable to identity thieves and other criminals. Defendants also knew of the serious harms that could happen if the PII of Plaintiff and the Class was wrongfully disclosed, that disclosure was not fixed, or Plaintiff and the Class were not told about the disclosure in a timely manner.

82. By being entrusted by Plaintiff and the Class to safeguard their Private Information, Defendants had a special relationship with Plaintiff and the Class. Plaintiff and the Class signed up for and paid for Defendants' services and/or products and agreed to provide their Private Information with the understanding that Defendants would take appropriate measures to protect it, and would inform Plaintiff and the Class of any breaches or other security concerns that might call for action by Plaintiff and the Class. But, Defendants did not.

83. Defendants breached their duty to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class Members' Private Information by failing to adopt, implement, and maintain adequate security measures to safeguard that information, despite repeated failures and intrusions, and allowing unauthorized access to Plaintiff's and the other Class Members' Private Information.

84. Defendants' failure to comply with industry and federal regulations further evidences Defendants' negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class Members' Private Information.

85. But for Defendants' wrongful and negligent breach of its duties owed to Plaintiff and the Class, their Private Information would not have been compromised, stolen, and viewed by unauthorized persons. Defendants' negligence was a direct and legal cause of the theft of the Private Information of Plaintiff and the Class and all resulting damages.

86. The injury and harm suffered by Plaintiff and the Class members was the reasonably foreseeable result of Defendants' failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the other Class members' Private Information. Defendants knew their systems and technologies for processing and securing the Private Information of Plaintiff and the Class had numerous security vulnerabilities.

87. As a result of this misconduct by Defendants, the Private Information of Plaintiff and the Class were compromised, placing them at a greater risk of identity theft and subjecting them to identity theft, and their Private Information was disclosed to third parties without their consent. Plaintiff and Class members also suffered diminution in value of their Private Information in that it is now easily available to hackers on the dark web. Plaintiff and the Class have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

88. Defendants' misconduct as alleged herein is malice or oppression, in that it was despicable conduct carried on by Defendants with a willful and conscious disregard of the rights or safety of Plaintiff and the Class and despicable conduct that has subjected Plaintiff and the

Class to cruel and unjust hardship in conscious disregard of their rights.

COUNT II – NEGLIGENCE *PER SE*
(On behalf of Plaintiff and the Class)

89. Plaintiff repeats, realleges, and incorporates by reference the allegations contained in paragraphs 1 through 78 as though fully stated herein.

90. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

91. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of PII it obtained and stored (of over one million current and former customers), and the foreseeable consequences of a data breach at a nationally-chartered bank as large as SouthState Bank, including, specifically, the immense damages that would result to Plaintiff and Class members.

92. Defendants' violation of Section 5 of the FTC Act constitutes negligence *per se*.

93. Plaintiff and Class members are within the class of persons that the FTC Act was intended to protect.

94. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

95. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and the Class have suffered, and continue to suffer, injuries and damages arising from identity theft;

Plaintiff's inability to use his debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charged and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives, including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports, and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

96. Additionally, as a direct and proximate result of Defendants' negligence *per se*, Plaintiff and Class members have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information in their continued possession.

COUNT III – BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff and the Class)

97. Plaintiff repeats, realleges, and incorporates by reference the allegations contained in paragraphs 1 through 78 as though fully stated herein.

98. Plaintiff and Class Members who made entered into services with SouthState Bank during the period in which the Data Breach occurred had implied contracts with Defendants.

99. Specifically, Defendants invited Plaintiff and Class members to purchase banking and financial services and products using their credit or debit cards. Plaintiff and Class Members

accepted Defendants' offers.

100. Plaintiff and Class Members paid money to Defendants and, in connection with those transactions, provided Defendants' with their card information and other Private Information. In exchange, Defendants agreed, among other things:

a. to provide banking and financial services or products to Plaintiff and Class Members;

b. to take reasonable measures to protect the security and confidentiality of Plaintiff's and Class Members' Private Information;

c. to protect Plaintiff's and Class Members' Private Information in compliance with federal and state laws and regulations and industry standards, and

d. to accurately and promptly notify Plaintiff and Class Members if their data had been breached or compromised.

101. Protection of Private Information is a material term of the contracts between Plaintiff and Class Members, on the one hand, and Defendants, on the other hand. Had Plaintiff and Class Members known that Defendants did not adequately protect customer Private Information, they would have never made engaged in commerce with Defendants.

102. Defendants did not satisfy their promises and obligations to Plaintiff and Class Members under the contracts in that it did not take reasonable measures to keep Plaintiff's and Class Members' Private Information secure and confidential and did not comply with the applicable laws, regulations, and industry standards. Defendants materially breached their contracts with Plaintiff and Class Members by failing to implement adequate security measures to protect Private Information.

103. Defendants further breached their contracts with Plaintiff and Class Members by

failing to provide timely and accurate notice to them that their Private Information was compromised in and as a result of the Data Breach.

104. Plaintiff and Class Members fully performed their obligations under their contracts with Defendants.

105. Defendants' failure to satisfy their obligations led directly to the successful breach of its computer servers and stored Private Information, in which Defendants let unauthorized parties access and exfiltrate Plaintiff's and Class Members' Private Information.

106. Defendants breached these contracts as a result of their failure to implement security measures.

107. Also as a result of Defendants' failure to implement the security measures, Plaintiff and Class Members have suffered actual damages resulting from the theft of their personal information and remain at imminent risk of suffering additional damages in the future.

108. Accordingly, Plaintiff and Class Members have been injured as a proximate result of Defendants' breaches of contract, sustained actual losses and damages as described above, and are entitled to damages and/or restitution in an amount to be proven at trial.

COUNT IV – UNJUST ENRICHMENT
(On behalf of Plaintiff and the Class)

109. Plaintiff repeats, realleges, and incorporates by reference the allegations contained in paragraphs 1 through 78 as though fully stated herein.

110. Plaintiff and Class Members conferred a monetary benefit upon Defendants in the form of monies paid for the purchase of banking and financial products and services.

111. Defendants appreciated or had knowledge of the benefits conferred upon them by Plaintiff and Class Members. Defendants also benefited from the receipt of Plaintiff's and Class Members' financial information.

112. The monies for banking and financial products and services that Plaintiff and Class Members paid to Defendants were supposed to be used by Defendants, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

113. As a result of Defendants' conduct, Plaintiff and Class Members suffered actual damages in an amount equal to the difference in value between the financial and banking products and services with the reasonable data privacy and security practices and procedures that Plaintiff and Class Members paid for, and the inadequate products and services without reasonable data privacy and security practices and procedures that they received.

114. Under principles of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiff and Class Members because Defendants failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiff and Class Members paid for and that were otherwise mandated federal, state and local laws, and industry standards.

115. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds received by it as a result of the conduct and data breach alleged herein.

COUNT V – BREACH OF CONFIDENCE
(On behalf of Plaintiff and the Class)

116. Plaintiff repeats, realleges, and incorporates by reference the allegations contained in paragraphs 1 through 78 as though fully stated herein.

117. At all times during Plaintiff's and Class Members' interactions with Defendants, Defendants were fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' Private Information that Plaintiff and Class Members provided to Defendant.

118. As alleged herein and above, Defendants' relationship with Plaintiff and Class Members was governed by expectations that Plaintiff's and Class Members' Private Information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

119. Plaintiff and Class Members provided their respective Private Information to Defendants with the explicit and implicit understandings that Defendants would protect and not permit the PII to be disseminated to any unauthorized parties.

120. Plaintiff and Class Members also provided their respective Private Information to Defendants with the explicit and implicit understanding that Defendants would take precautions to protect that PII from unauthorized disclosure, such as following basic principles of information security practices.

121. Defendants voluntarily received in confidence Plaintiff's and Class Members' Defendants' with the understanding that the information would not be disclosed or disseminated to the public or any unauthorized third parties.

122. Due to Defendants' failure to prevent, detect, and/or avoid the Data Breach from occurring by, *inter alia*, failing to follow best information security practices to secure Plaintiff's and Class Members' Private Information, Plaintiff's and Class Members' Private Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

123. As a direct and proximate cause of Defendants' actions and/or omissions, Plaintiff and Class Members have suffered damages.

124. But for Defendants' disclosure of Plaintiff's and Class Members' Private Information in violation of the parties' understanding of confidence, their Private Information

would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendants' Data Breach was the direct and legal cause of the theft of Plaintiff's and Class Members' Private Information, as well as the resulting damages.

125. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Defendants' unauthorized disclosure of Plaintiff's and Class Members' Private Information. Defendants knew its computer systems and technologies for accepting and securing Plaintiff's and Class Members' Private Information had numerous security vulnerabilities because Defendants failed to observe industry standard information security practices, including Defendants' inability to detect the Data Breach.

126. As a direct and proximate result of Defendants' breaches of confidence, Plaintiff and the Class have suffered, and continue to suffer, injuries and damages arising from identity theft; Plaintiff's inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charged and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives, including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports, and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

127. As a direct and proximate result of Defendants' breaches of confidence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm,

including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT VI – VIOLATION OF THE SOUTH CAROLINA DATA BREACH SECURITY ACT, S.C. Code Ann. §§ 39-1-90
(On behalf of Plaintiff and the South Carolina Subclass)

128. Plaintiff repeats, realleges, and incorporates by reference the allegations contained in paragraphs 1 through 78 as though fully stated herein.

129. The South Carolina Data Breach Security Act (the "Act") requires persons conducting business in this State and owning, licensing or maintaining computerized data that includes personal identifying information to disclose breaches of the security of the system to those affected. This required disclosure "must be made in the most expedient time possible and without reasonable delay . . . ." S.C. Code Ann. § 39-1-90(A).

130. Defendants are "persons" as defined by the statute. S.C. Code Ann. § 39-1-90(D)(2).

131. As described more fully above, Defendants conduct business in this State and owns, licenses or maintains computerized data that includes personal identifying information.

132. Plaintiff's and Class Members' Private Information compromised in the Data Breach meets the definition of "personal identifying information" in the statute. S.C. Code Ann. § 39-1-90(D)(3).

133. The Data Breach meets the definition of "Breach of the security of the system" in the statute. S.C. Code Ann. § 39-1-90(D)(1).

134. Defendants violated the Act by unreasonably delaying disclosure of the Data Breach to Plaintiff and Class Members whose Private Information was, or was reasonably believed to have been, acquired by an unauthorized third person.

135. Defendants knew or should have known that it was violating South Carolina law

by unreasonably delaying disclosure of the Data Breach. This renders Defendants' violation of the Act willful and knowing.

136. Upon information and belief, no law enforcement agency determined that notification to Plaintiff and Class Members would impede a criminal investigation.

137. As a result of Defendants' violation of the Act, Plaintiff and Class Members suffered and will continue to suffer damages and injury set forth above.

138. Plaintiff and Class Members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, restitution, injunctive relief, attorneys' fees, and any other relief that is just and proper.

COUNT VII – DECLARATORY/INJUNCTIVE RELIEF
(On behalf of Plaintiff and the Class)

139. Plaintiff repeats, realleges, and incorporates by reference the allegations contained in paragraphs 1 through 78 as though fully stated herein.

140. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court may enter a judgment declaring the rights and legal relations of the Parties and grant further necessary relief. The Court also has broad authority to restrict acts that are tortious and violate the terms of regulations described in this Complaint.

141. There is an actual, substantial controversy concerning Defendants' present and prospective obligations to reasonably protect customers' Private Information and whether Defendant is upholding cybersecurity measures sufficient to protect the Class, including Plaintiff, from future security breaches that risk Plaintiff's and Class Member's information.

142. Plaintiff avers that Defendants' cybersecurity measures are insufficient. Also, Plaintiff and Class Members still suffer injury from the Data Breach and stay at imminent risk that future breaches of their private information and ongoing fraud against them will happen.

143. Plaintiff petitions the Court to enter a judgment declaring the following: (i) Defendants owe a duty to protect consumers' private information and to timely notify them of a data breach under common law, South Carolina statutory law, and Section 5 of the FTC Act; and (ii) Defendants are in in violation of these legal duties by failing to impose reasonable measures to protect consumers' private information in its possession and control.

144. Plaintiff asks the Court to issue injunctive relief mandating Defendants to use appropriate security controls consistent with law and industry standards to safeguard consumers' private information from future data breaches.

145. If an injunction is not issued, the Class Members will suffer irreparable injury and lack a sufficient legal remedy, should another data breach at SouthState Bank occur. The risk of another breach is real, immediate and substantial. If another breach at SouthState Bank happens, the Class Members will not have an adequate legal remedy because several of the corresponding injuries are not readily quantified and Class Members will be compelled to bring several lawsuits to correct the same misconduct.

146. The hardship to Class Members if an injunction is not granted exceeds the hardship to Defendants if an injunction is granted. If a similar security breach happens again from Defendants' repeated misconduct, Class Members likely will be subjected to substantial hacking attempts and other damage. The cost to Defendants of complying with an injunction by imposing reasonable cybersecurity standards is minimal, and Defendants have pre-existing legal duties to impose such measures.

147. Issuance of the petitioned injunction will not harm the public interest, Rather, such an injunction would behoove the public by precluding further data breaches at SouthState

Bank, thereby eliminating the additional injuries that would result to the Class Members and the millions of consumers whose private information would be further at risk.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other Class members, respectfully requests this Court enter an Order:

(a) Certifying the United States Class, and appointing Plaintiff as Class Representatives;

(b) Finding that Defendants' conduct was negligent, deceptive, unfair, and unlawful as alleged herein;

(c) Enjoining Defendant from engaging in further negligent, deceptive, unfair, and unlawful business practices alleged herein;

(d) Awarding Plaintiff and the Class members actual, compensatory, and consequential damages;

(e) Awarding Plaintiff and the Class members statutory damages and penalties, as allowed by law;

(f) Awarding Plaintiff and the Class members restitution and disgorgement;

(g) Requiring Defendant to provide appropriate credit monitoring services to Plaintiff and the other class members;

(h) Awarding Plaintiff and the Class members punitive damages;

(i) Awarding Plaintiff and the Class members pre-judgment and post-judgment interest;

(j) Awarding Plaintiff and the Class members reasonable attorneys' fees costs and expenses, and;

(k) Granting such other relief as the Court deems just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Respectfully Submitted,

Dated: April 12, 2024

/s/ Stuart H. McCluer

Stuart H. McCluer (Federal ID No. 13213)
McCulley McCluer LLC
701 E. Bay St., Suite 411
Charleston, SC 29403
(843) 444-5404
smccluer@mcculleymccluer.com

Jean S. Martin
(*Pro Hac Vice application forthcoming*)
Francesca K. Burne
(*Pro Hac Vice application forthcoming*)
Morgan & Morgan Complex Litigation Group
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 223-5505
jeanmartin@ForThePeople.com
fburrne@ForThePeople.com